REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YYYY) 12-06-2015	2. REPORT TYPE Master's Thesis	3. DATES COVERED (From - To) 21-7-2014 to 12-06-2015

4. TITLE AND SUBTITLE	
The Panacea and the Square Peg: Strategic Fallacies of the Air, Undersea and Cyber Domains	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	
John C. Witte Lieutenant Commander, United States Navy	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT
Joint Forces Staff College Joint Advanced Warfighting School 7800 Hampton Blvd Norfolk, VA 23511-1702	

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited

13. SUPPLEMENTARY NOTES
Not for Commercial Use without the express written permission of the author

14. ABSTRACT
Strategic thought about new domains can fall victim to logical fallacies. In the interwar period between WWI and WWII, overestimating the impact of air power led strategist to view this new capability as a panacea. For the undersea domain, strategists ignored both the technical limitations that prevented submarines from performing traditional maritime warfare roles and the unique possibilities presented by the elements of stealth and surprise. The square peg fallacy illustrates the strategic effect of wedging submarines into the dominant naval strategy of major fleet engagement.

Current thought on the use of cyber power appears susceptible to both fallacies. Mirror imaging the potential effects of a cyber-attack on the US leads some strategists to overestimate the strategic effects of cyber power. The Air-Sea Battle Concept demonstrates the square peg fallacy in how it advocates cyber operations as a method to defeat air defenses. Based on historical analysis, recommendations for future cyber strategy include: conducting defensive cyber operations under the joint function of protection, controlling offensive cyber operations in a manner similar to special operations, and utilizing cyber power's unique advantages against non-state actors.

15. SUBJECT TERMS
Domains, Strategy, Air Power, Undersea Warfare, Submarines, Cyber Power, Interwar Period, Innovation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Unclassified Unlimited	50	19b. TELEPHONE NUMBER (include area code) 757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

**THE PANACEA AND THE SQUARE PEG: STRATEGIC
FALLACIES OF THE AIR, UNDERSEA, AND CYBER DOMAINS**

by

John C. Witte

Lieutenant Commander, United States Navy

i

THIS PAGE LEFT INTENTIONALLY BLANK

THE PANACEA AND THE SQUARE PEG: STRATEGIC FALLACIES OF THE AIR, UNDERSEA, AND CYBER DOMAINS

by

John C. Witte
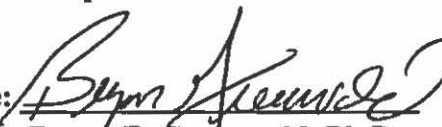
Lieutenant Commander, United States Navy

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.
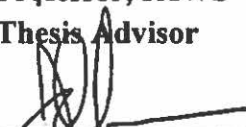
Signature: _____

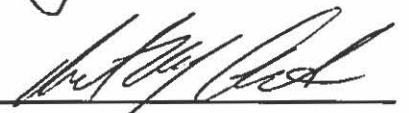John C. Witte, LCDR, US Navy

21 April 2015

Thesis Advisor: Signature: _____

Bryon E. Greenwald, Ph.D.
Professor, JAWS
Thesis Advisor

Approved by: Signature: _____

Doug Golden, Colonel, US Air Force
Committee Member

Signature: _____

Dr. Robert Antis, Ph.D.
Director, Joint Advanced Warfighting School

i

ABSTRACT

Strategic thought about new domains can fall victim to logical fallacies. In the interwar period between WWI and WWII, the exhilarating idea of invulnerable bombers beating opposing nations into submission masked significant miscalculations inherent in Allied air power theory and led strategist to view this new capability as a panacea. For the undersea domain, strategists ignored both the technical limitations that prevented submarines from performing traditional maritime warfare roles and the unique possibilities presented by the elements of stealth and surprise. The square peg fallacy illustrates the strategic effect of wedging submarines into the dominant naval strategy of major fleet engagement.

Current thought on the use of cyber power appears susceptible to both fallacies. Mirror imaging the potential effects of a cyber-attack on the US leads some strategists to overestimate the strategic effects of cyber power and envision the domain as a panacea through which to dominate future conflicts. The Air-Sea Battle Concept demonstrates the square peg fallacy in how it advocates cyber operations as a method to defeat air defenses, a problematic approach that fails to consider significant technical limitations. Based on historical analysis, recommendations for future cyber strategy include: conducting defensive cyber operations under the joint function of protection to more realistically view US capabilities and vulnerabilities, controlling offensive cyber operations in a manner similar to special operations (a construct that more closely matches its potential battlefield effects), and utilizing cyber power's unique advantages against non-state actors.

DEDICATION

Dedicated to my wife and kids (the ultimate Navy family) and the Fightin'
Shipmates of Seminar One.

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

The opportunity to exploit a new domain of warfare presents a blank canvas to military strategists. But the relative freedom of unexplored territory can just as easily yield a costly mess as a strategic masterpiece. This creative process played out in the evolution of strategic bombing for the air domain and unrestricted submarine warfare during the interwar period between World War I and World War II. In the air domain, the exhilarating idea of invulnerable bombers beating opposing nations into submission masked significant miscalculations inherent in Allied air power theory. Strategists overestimated the operational effect of fighting in the air and viewed this new capability as a panacea to cure the stalemate of World War I. For the undersea domain, strategists attempted to work submarine power into the dominant naval theory of concentrating forces for a decisive battle. This concept ignored both the technical limitations that prevented submarines from effectively participating in that strategy and the unique possibilities presented by the elements of stealth and surprise. Eventually, submarines would influence the war through a strategy of dispersion, avoiding opposing naval forces and attacking the enemy's economy by sinking commercial vessels. This action only became possible when strategists realized that the submarine was a square peg that would not fit into the round hole of established naval strategy. Effective exploitation of both air and undersea domains required overcoming fallacies in strategic thought.

The divergent development of air and submarine strategies prior to WWII provides an instructive example to guide cyber strategy as it develops to meet future threats. Current thought on the use of cyber power appears susceptible to the fallacious logic represented by the ideas of the panacea and square peg. Some theorists envision the cyber domain as the

predominant battlefield for future conflicts, or even the only battlefield.[1] Others confine the cyber domain to a construct that supports traditional warfighting ideas while failing to capitalize on its unique characteristics.[2] By applying the historical lessons of air and undersea combat development, cyber theory can avoid the fallacies and paint a more strategically coherent picture of security in this new domain.

Foundations in Theory

The balance of this chapter provides the theoretical basis and starting point for this argument. It defines domains and their place in joint doctrine and introduces the unique challenges of developing strategy for a new domain. The narrative continues by relating the constructs of the panacea and square peg to established logical fallacies. The chapter ends with an introduction of how each of the fallacies influenced early strategy in the air and undersea domains.

Defining Domains and Domain Concept

The definition of an operational domain becomes more complex as technology introduces new types of warfare into the joint world. Joint doctrine specifies four physical domains (land, maritime, air and space) and includes cyberspace as a domain of the information environment.[3] The advantage of this construct is that it differentiates cyberspace

---

[1] David J. Lonsdale, *The Nature of War in the Information Age*, (New York: Frank Cass Publishing, 2004), 2. Lonsdale describes the views of several leading theorists, with prolific technology writer Winn Schwartau taking the most extreme view of future cyber dominance. Admiral William Owens' "system of systems" view of battlespace awareness and Martin Libicki's "mesh" construct further emphasize the role of cyberspace in military operations.

[2] E. Lincoln Bonner III, "Cyber Power in 21st Century Joint Warfare," *Joint Forces Quarterly*, 74, (3rd Quarter 2014): 72. Bonner advocates the idea of "cyber superiority" and "cyber interdiction", geographic concepts that associate cyber operations with traditional warfare roles.

[3] US Joint Chiefs of Staff, *Joint Operations Planning*, Joint Publication 3-0, (Washington, DC: Joint Chiefs of Staff, 11 August 2011), IV-1, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (accessed January 28, 2015).

from the physical domains and attempts to preempt poor analogies to geographic concepts (e.g., mass and maneuver in cyberspace). However, by including cyber in the information operations environment, joint doctrine groups it with abstract cognitive concepts like the decision making process of senior leaders and shared beliefs of other nations.[4] While information operations of that sort can be quite powerful, they have little in common with technically demanding disciplines like computer network defense other than the general idea that both activities involve information. This ill-fitting categorization obscures the strategic potential of cyber power. The electronic links between geographically distant systems and the near-instantaneous transmission of information render cyberspace essentially place-less, which tends to complicate strategic thought. While air and undersea operations introduced a third dimension to warfare (depth and altitude), cyber operations see essentially no difference between networked computers in the same building and networked computers separated by 2000 miles. A more comprehensive idea of what constitutes a domain may serve to bridge the gap.

There is little disagreement that land constitutes the original domain for conflict. By adopting Clausewitz's definition of warfare as policy continued by other means, specifically violent conflict, one can reasonably define land warfare. All other domains can be thought of in terms of their differences from warfare on land. With the advent of ships, aircraft and spacecraft, new venues for warfare or the continuation of policy through violence emerged. What differentiates the sea, air, and space as domains distinct from the land domain is the fact that they are inaccessible for strategic use without enabling technology. As a result, an

---

[4] US Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, DC: Joint Chiefs of Staff, 27 November 2012 incorporating Change 1 of 20 November 2014) I-5, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed January 28, 2015).

appropriate definition of a domain (other than the land domain) is: a medium for violent conflict to further policy that is accessible only through distinct technological means.

Does cyberspace meet this definition? Computer networks form the access point to (and largely make up) the domain, and it is a venue for conflict through cyber-attacks. It is violent in the sense that adversaries can destroy valuable and strategically important property (systems and data) and they could potentially hurt people through indirect means like cyber-induced power grid failure. By including violent conflict in the definition, cyberspace fits more logically in the domain category and is more easily distinguished from the general category of information environment.

This definition also proves useful in understanding the strategic differences between undersea and surface naval operations. Joint Doctrine does not specify undersea warfare as its own domain, but the idea of violent conflict and distinct technology are worth discussing in this context. While both platforms can generate violent action, submarines (even the earliest designs) and surface ships use different technologies. The U.S. Navy's publication entitled Undersea Warfighting, a commander's guidance document for the submarine force, refers extensively to submarine operations as taking place in the undersea domain, separate from the rest of the maritime domain.[5] It may not be useful for joint publications to observe this differentiation because the domain is only used by one component of one service. But the division is useful in light of the strategic misconceptions that accompanied the early use of submarines in war, and that now appear to affect the use of cyber power.

---

[5] Commander Submarine Forces, *Undersea Warfighting*, (Norfolk, VA, July 2011), 8.

4

Logical Fallacies and New Domains

The idea of a panacea, or cure-all, derives from mankind's conception of both hope and fear. The hope comes from the promise of a better life and the fear results from thoughts of suffering and death. The thought that military operations in a new domain might promise a quick end to wars and deliver the nation from terrifying consequences is an example of the logical fallacy of appealing to emotion. Specifically, an appeal to emotion is an attempt to arouse the emotions of the audience to gain acceptance of a conclusion.[6] The fact that the audience deeply desires something to be true does not mean it is true. Interwar air power theorist Major General James E. Fechet demonstrated this line of thinking when he speculated in 1933 that New York City could be razed to the ground and depopulated in a single day by attack from the air.[7] This image, although not particularly supported by the technical capabilities of aviation at the time, created a visceral image in the minds of the audience that lent credence to the idea that air warfare is both a crucial vulnerability and a powerful tool that will dominate future wars.

While the panacea fallacy assigned fantastic new possibilities to the air domain, square peg thinking relegated undersea warfare to just "more of the same". Early thought on the use of submarines concentrated on how the world's navies could integrate them into existing naval theory. This unimaginative thinking was symptomatic of the fallacy of division. This fallacy asserts that if a whole has certain qualities, all parts of the whole have the same qualities.[8] The key organizing concept of traditional maritime strategy in period during which submarines first

---

[6] T. Edward Damer, *Attacking Faulty Reasoning: A Practical Guide to Fallacy-Free Arguments (Seventh Edition)*, (Boston, MA: Wadsworth, 2013), 44-56.
[7] Philip Meilinger, editor. *The Paths of Heaven: The Evolution of Airpower Theory*, (Maxwell AFB, AL: Air University Press, 1997), 470.
[8] Damer, *Attacking Faulty Reasoning*, 151.

emerged was the fleet-on-fleet engagement. Undersea warfare was seen as a part of maritime warfare and therefore its organizing strategy should also focus on fleet-on-fleet engagements. In 1939, the US naval doctrine publication *Current Doctrine, Submarines* mandated: "The primary task of the submarine is to attack enemy heavy ships. A heavy ship is defined as a battleship, a battle cruiser, or an aircraft carrier."[9] This task ignored the significant technical limitation of low submerged speed and the advantages of stealth. The square peg fallacy led naval strategists to apply the new tool of submarines in the same way as any other tool at their disposal, ignoring the possibility of bypassing the enemy's naval forces and attacking his economy directly.

Shortcomings of Domain Strategy

The disruptive effect of new domains comes from the possibility of negating underlying assumptions of strategy. The mobility of an aircraft and the absence of opposing lines of battle or geographic barriers led early theorists to assume that air power's defining characteristic was unstoppable offense. But the exhilarating possibilities of this newly-accessible third dimension kept theorists from understanding what an air defense system might look like. Early air power theorist Giulio Douhet understood this new technology to require a wholesale revision of strategic thought. Unfortunately, his influence steered initial air strategy towards the panacea fallacy.

Although submarines only became useful as warships towards the very end of Alfred Thayer Mahan's life, neither, influential naval theorist, he nor his adherents saw any reason that operations under the waves would be much different strategically than operations on the

---

[9] Randy Papadopoulos, "Between Fleet Scouts and Commerce Raiders", *Undersea Warfare,* 7, no.4 (Spring 2005): 26.

surface. Submarines of that era had significant technical limitations. Their weapons systems did not have the striking power or accuracy necessary to sink top of the line warships, and their submerged speed was not sufficient to position themselves to attack steaming formations of warships. These limitations did not allow submarines to be a part of massive fleet-on-fleet action. The submarine's strength lay in the very antithesis of this idea. The lack of innovative thinking drove undersea domain strategy towards the square peg fallacy.

Theories on the use of cyber power have exhibited errors on both extremes. Some thinking tends to emphasize offensive cyber operations and advocates it as an alternative to traditional warfare. Some authors even compare cyber operations to nuclear weapons due to their perceived unstoppable offense capability.[10] Other strategists view cyber warfare in the combined arms construct, as a tool for each combatant commander to use alongside conventional forces. This approach ignores the stealth and secrecy aspects that cyber shares with undersea operations. The Department of Defense continues to prioritize funding for cyber operations, instituting an 8.5% increase to $5.1 billion in 2015 despite implementing significant cuts in most other spending.[11] In an era of diminishing defense budgets, it is vital that senior defense leaders have a better understanding of the strengths and weakness of the cyber domain to make resource decisions that are unclouded by fallacious ideas.

The enduring power of logical fallacies comes from their ability to simplify complex issues into comfortable generalizations. The panacea fallacy tapped into the disgust and horror

---

[10] Matthew D. Crosston, "World Gone Cyber MAD," *Strategic Studies Quarterly*, 5, issue 1 (Spring 2011): 100. This idea is also discussed extensively by Colin Gray in his monograph "Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling".

[11] Dennis Murphy, "Pentagon Budget 2015: DoD Cyberspace Operations Would Get 8.5% Boost", *Janes*, March 16, 2014, http://www.janes.com/article/35427/pentagon-budget-2015-dod-cyberspace-operations-would-get-8-5-boost (accessed February 2, 2015).

prevalent in western nations after WWI and presented air power as a wholly separate alternative containing none of the problematic issues of land warfare. The square peg fallacy put off any serious consideration of the disruptive effects of submarine operations in favor of the widely accepted conventional wisdom of the day. Poor strategic assumptions on operations in the air and undersea domains led strategists in WWII to make decisions that were extremely costly in both equipment and human lives. By recognizing these assumptions as the result of logical fallacies, strategists can avoid making similar mistakes when planning for operations in the cyber domain.

CHAPTER 2: AIR DOMAIN CASE STUDY - SOARING ABOVE STALEMATES AND STRIKING CITIES

This chapter demonstrates the panacea fallacy by analyzing the critical flaws in early in WWII Allied air power theory. Specifically, the belief that air power heavily favored the offense led Allied leaders to erroneously prioritize bomber operations against Germany during the Combined Bomber Offensive. The ability to target the enemy's industrial centers and population gave the false hope that operations in the new domain would avoid the slaughter and stalemate of the WWI trenches and might even make a land invasion unnecessary. The chapter concludes by exploring evidence of the panacea fallacy in the cyber domain.

The Bomber Will Always Get Through

The bloody conclusion of WWI left all sides looking for a new way of war that would avoid the ghastly attrition of trench warfare. Industrial-scale bombardment from the air held the promise of resolving conflicts quickly. Air power advocates asserted that air warfare would make all other forms of combat obsolete, an appealing concept that would reappear over the next hundred years with the advent of nuclear weapons and even cyber power.

In his influential work on early air power theory, Giulio Douhet argued that it was now possible to invade the enemy's territory without breaking through his defensive lines on the ground. He combined this idea with the notion that "nothing man can do on the surface of the earth can interfere with a plane in flight, moving freely in the third dimension."[1] These ideas

---

[1] Giulio Douhet, *The Command of the Air*, translated by Dino Ferrari (Washington, DC: Office of the Air Force History, 1983, originally published 1942), 9; David MacIsaac, "Voices of the Central Blue: The Airpower Theorists," in Peter Poret, ed. *Makers of Modern Strategy: From Machiavelli to the Nuclear Age,* (Princeton, NJ: Princeton University Press, 1986), 624-647.

were problematic, even given what was known about air warfare at the time. WWI air combat showed that once aircraft invaded the enemy's territory, defensive counterattacks by the enemy's aircraft could complicate things immensely. Douhet also assumed that there would be significant breakthroughs in aircraft technology, while ground-based anti-aircraft systems would largely remain ineffective. Finally, his theory of the offensive dominance of air power was based on the notion that the enemy could not defend all areas from air attack continuously. Douhet firmly believed that attacking a nation's civilian population and wartime economy from the air would destroy the will to wage war quickly. As the Allies discovered in WWII, however, it was possible to establish an effective air defense around vital infrastructure, and there were vast areas of each country that, if bombed, would not harm the nation's ability to wage war in the least. But Allied war planners embraced his ideas, assigning strategic bombing as the dominant role for air power in WWII.

Douhet's theories contained an important and ultimately quite costly corollary: if ground-based air defenses were ineffective in stopping bombing attacks, so too were enemy defensive fighters. This, the bomber, in formation, would provide its own defense and be unstoppable. This concept became a founding idea for Allied air power doctrine and supplied the context for the oft-repeated quote by Tory leader Stanley Baldwin in 1932 that proclaimed to the man in the street that "there is no power on earth that can protect him from being bombed. Whatever people may tell him, the bomber will always get through ..."[2] The U.S. Army Air Forces (USAAF), specifically the Eighth Air Force, translated this concept into unescorted daylight bombing raids over Germany only to suffer heavily from *Luftwaffe* flak and defensive fighter swarms. The "Mighty Eighth" suffered horrific losses during the

---

[2] Paul Kennedy. *Engineers of Victory*, (New York: Random House, 2013), 85.

Combined Bomber Offensive, including over 50% of airframes on October 12, 1944, the "Black Thursday" raid over Schweinfurt. Sadly, it took such losses to convince air commanders that this theory was tragically false. Only with the introduction of drop tanks and the P-51 Mustang long range fighter escort did the Allies fend off *Luftwaffe* defensive counter-air attacks sufficiently to continue offensive bombing operations.[3]

During the Interwar period, the idea that bombers were unstoppable became firmly established among true believers in air power. Reinforcing this belief was the fact that the societal and governmental effects of bombing population centers were not testable in peacetime, leaving the strategic effects bombing unproven and largely a matter of belief. This led to a convergence of interests that drastically enhanced the power of the panacea fallacy. For Douhet, Billy Mitchell in the U.S. and Hugh Trenchard in Britain, it was vitally important that air forces achieve independence and recognition as a separate armed service. Strategic bombing provided a powerful justification for this arrangement. An independent air force would concentrate on bombing targets far from any associated ground troops towards independent objectives. The Air Corps Tactical School provided another layer panacea thinking by concentrating on the economic effects of bombing. The doctrine they developed in the Interwar period thought of the enemy society as an "industrial web" susceptible to collapse by targeting key nodes.[4] This mechanistic view of warfare reinforced the idea that indecisive, bloody stalemates on land were a thing of the past.

Once the idea of strategic bombing as a panacea took hold, it dominated the thinking of air strategists throughout WWII. However, the initial U.S. war planning did not reflect this

---

[3] Allan R. Millet and Williamson Murray, *A War To Be Won*, (Cambridge, MA: Belknap Press), 312-313.
[4] Mellinger, *The Paths of Heaven*, 476.

outlook. Rainbow 5, the Allied war plan in place at the time of U.S. entry into the war, directed "weakening the enemy's war-making powers by blockade and strategic bombing" only as preparation for an eventual invasion by land forces.[5] Sharing blockade responsibility with the navy was hardly the revolutionary role air power advocates envisioned for their independent force. The priority for the USAAF was to commence the buildup of bombers in the U.K. as soon as possible and conduct an extended bombing campaign against Germany; USAAF leadership would rally against any strategy that planned otherwise. Thus, the USAAF and the Eighth Air Force viewed the start of Operation Torch in North Africa as an unwelcome diversion of forces from what they saw as the main effort against Germany. USAAF commander General H. H. Arnold attempted bureaucratic maneuvers to consolidate all air forces in Europe and Africa under one commander, with the intent of having that commander prevent bombers from being taken out of their strategic bombing role.[6] That the senior U.S. air commander prioritized the strategic bombing mission against Germany over supporting active combat operations both in Africa and the Pacific is a strong indication of the deep entrenchment of the panacea fallacy.

Despite the initial instructions in Rainbow 5, advocates of strategic bombing would not cede its place as the preeminent idea in air power. At the Casablanca conference in January 1943, the Allies agreed to commence long-range bomber operations from the U.K. Two main points drove agreement on the Combined Bomber Offensive (CBO). That the Africa campaign was drawing to a close and there were not yet sufficient forces in England for the planned cross-channel invasion. The CBO seemed like the best, perhaps the only way, to keep pressure

[5] W. A. Jacobs, "Strategic Bombing and American National Strategy 1941-1943", *Military Affairs*, 50, no. 3 (July, 1986): 133.
[6] Ibid., 136.

on Germany and provide a second front, relieving the beleaguered Russian Army. The implementing direction to Allied air commanders contained the wording that moved air power in the direction envisioned by Douhet and Mitchell: "Your primary object will be the progressive destruction and dislocation of the German military, industrial and economic system, and the undermining of the morale of the German people to a point where their capacity for armed resistance is fatally weakened."[7] It was with this guidance that the greatest test of air domain theory began.

The CBO in Retrospect

The CBO began with hopes of bringing Germany to its knees without conducting a cross-channel invasion. This hope fell away quickly. The anticipated morale degradation and governmental paralysis from widespread bombing of cities never materialized, either from German bombing of London or Allied raids into Germany. The emphasis then shifted to bombing industrial targets, with the intent of grinding industry to a halt and destroying the enemy's war economy. This approach presented its own difficulties due to the imprecise nature of analyzing what industrial facilities were important. German machine tools, vital to industrial production, were quite numerous (greater than 2 million) and built solidly enough to withstand most bombing except a direct hit. Their storage locations had no obvious identifying characteristics visible from the air and as a result, Allied planes never bombed the vast majority of German buildings that housed them.[8] Even when the CBO changed priority to target German aircraft production, fighter production actually increased in 1944.[9]

---

[7] Jacobs, "Strategic Bombing and American National Strategy 1941-1943," 137.
[8] A. D. Harvey, "Air Power in Perspective", *Air Power History* (Fall 2013): 6.
[9] Lt Col Woody Paramore, "The Combined Bomber Offensive's Destruction of Germany's Refined Oil Industry" *Air and Space Power Journal* (March-April 2012): 81.

The CBO then shifted its target to gasoline and oil supplies. Although there is some debate about whether strategic bombing of oil production facilities or Allied occupation of Romanian oil fields was the decisive factor, it is safe to say that the CBO significantly degraded German oil production.[10] But this decrease alone did not have a decisive strategic effect. Analysis of the CBO ultimately credits it with causing brutal attrition of *Luftwaffe* pilots as they attempted to defend against the bombing onslaught, reducing combat strength by 40% in 1944 from its peak at the beginning of the war. Even this reduction was related to organizational choices by the Germans, who prioritized increasing tank crew numbers 300% during this same period in a similarly demanding discipline requiring comparable training time to aviation.[11]

The historical scorecard eventually credited the CBO with attrition of German pilots and reduction in oil industry capacity, resulting in anemic opposing air power during the landings at Normandy. The CBO is also credited with snarling the road and rail links to the battlefield, degrading Germany's ability to bring reinforcements to the front. Although important to the overall war effort, this is a far cry from the decisive results envisioned by early air power theorists. Once promising to do away with the bloody attrition of the trenches, the CBO just moved the attrition a few thousand feet upward with heavy losses of men and aircraft on both sides.

It is not difficult to see why Douhet thought that air power would change war forever. Without advances such as radar and integrated air defenses, it would be exceedingly difficult to stop inbound bombers. If one nation could maintain a substantial edge in aviation technology

---

[10] Paramore, 73.

[11] Harvey, 11.

for an extended period, they would have a sizeable military advantage over their opponent. But a recurring theme in the exploitation of new domains is that after an initial success by one side, competition soon follows. In the end, the ability to bypass land forces and strike inside an enemy's territory was only as good as the air forces' ability to evade or defeat the enemy's defenses, select the right targets, and strike them accurately with enough force to destroy them. Air forces in WWII experienced varying degrees of difficulty achieving some or all of these requirements. With each added layer of complexity, the hope of a panacea receded further.

The Panacea Fallacy in the Cyber Domain: A Gateway to Quick and Efficient Victory?

As was the case with air power, the cyber domain affords the opportunity to attack adversaries and defend against attacks by them in a completely new setting. The unique characteristics of the domain (most of the action takes place within computer networks) lead some to believe that accomplishing the political objectives of war is possible primarily through that domain without the wholesale death and destruction that has accompanied war throughout history. This appeal to hope in place of reason is the heart of the panacea fallacy.

The thought of cyber power as a panacea derives considerable strength from mirror imaging. Former Secretary of Defense Leon Panetta asserted that the vulnerability of U.S. infrastructure to cyber-attack could lead to a "cyber-Pearl Harbor".[12] In *Cyberwar*, Richard Clarke plunges the US into an apocalyptic nightmare, complete with gas refinery explosions, trains crashing into each other, and economic collapse due to the hypothetical actions of Chinese hackers.[13] The vision of extensive communication and power grid failures delivered

---

[12] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack," *New York Times*, October 11, 2012.

[13] Richard Clarke and Robert Knake. *Cyber War*, (New York: HarperCollins, 2010), 64.

via the cyber domain are much more plausible (and therefore more terrifying) to the public than the extremely unlikely scenario of the same effects delivered via airborne bombardment. All of this serves to enhance the perceived power of the cyber domain. If the US was this vulnerable, could the military use the same vulnerabilities against potential adversaries?

The thought of turning off all electrical power and stopping all telecommunications in an adversary nation is indeed appealing. By using the cyber domain, it is theoretically possible to achieve effects that previously required weeks of bombing or a full scale invasion. But even while ignoring the significant technical challenges associated with achieving that far-reaching result through cyber power, several problems remain. The cyber-attack has answered the question of "ways", but what of the "ends"? Even if the enemy achieves this effect, the loss of power and communication are likely to be temporary, on the order of hours or days instead of weeks.[14] Without follow-up operations in the air and land domains (with their accompanying death and destruction) it is unlikely that the loss of power and communication alone would coerce an adversary to accede to US policy demands.

Remaining hopes for a rapid, bloodless victory through cyber power center around deterrence. Some theorists compare cyber capabilities to nuclear weapons and propose using them to create a "mutually assured cyber-destruction" balance of power to promote peace.[15] This too is problematic. Although information systems are vulnerable to cyber-attack, threatening to do so increases the probability that the adversary will make efforts to shore up these vulnerabilities. Even if the threat of severe cyber-attacks could never be overcome,

---

[14] Erik Gartzke, "The Myth of Cyberwar", *International Security,* 38, no. 2 (Fall 2013): 58.
[15] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute, April 2013): 5.

companies and organizations could make the decision to move all their operations off networks and into closed systems, basically setting economies back to where they were in 1995 before the Internet became a prevalent part of everyday life.[16] Life in 1995 America, although more inconvenient than life today, is hardly comparable to the aftereffects of a nuclear bomb. Attribution poses a problem as well. The frequently anonymous nature of cyber-attacks prevents the assured retaliation necessary for deterrence to work. This environment makes it unlikely that US cyber power can even deter other nations from using cyber weapons, much less any other sort of aggressive action.

The December 2014 cyber-attack against Sony Pictures illustrated several major flaws in the idea of cyber power as a panacea. Attribution was initially a problem, with the US waiting several weeks to accuse North Korea of orchestrating the attacks and North Korea subsequently denying responsibility.[17] President Obama publicly announced that the US would issue a "proportional response" and North Korea then completely lost its limited Internet connectivity for over nine hours with sporadic failures after that. North Korea blamed the US for the outage, but the US did not claim responsibility.[18] The US later issued economic sanctions on three North Korean government entities and ten individuals, a small gesture when added to the extensive network of sanctions already in place. The probable (but officially denied) use of cyberweapons by both sides and subsequent quick return to the status quo makes

[16] Martin C. Libicki, "Why Cyber Will Not and Should Not Have Its Grand Strategist", *Strategic Studies Quarterly*, 8, issue 1 (Spring 2014): 32.

[17] David E. Sanger and Nicole Perlroth, "US Said to Find North Korea Ordered Cyber Attack on Sony" *New York Times*, Dec 17th, 2014.

[18] Jack Kim, "North Korea Blames US for Internet Outages, Calls Obama 'Monkey'", *Reuters.com*, December 27, 2014, http://www.reuters.com/article/2014/12/27/us-northkorea-cybersecurity-idUSKBN0K502920141227 (accessed January 2, 2015).

cyber-deterrence arguments increasingly hard to justify. Even finding an accurate way to describe the event is challenging.

Defining this cyber-attack as warfare presents problems. President Obama classified the attack as "cyber vandalism".[19] The event was an attack by another nation on a Japanese-owned company that creates movies in America. There was extensive data loss, executives were embarrassed by the publishing of confidential emails, and several unreleased movies were leaked on the Internet, potentially lowering their box office returns. The hackers posted threatening messages invoking terrorism that ultimately caused Sony to cancel (and later reschedule) the theater release of "The Interview", a comedy featuring the assassination of an actor playing North Korean leader Kim Jung Un (in notes left by the hackers the movie was cited as the provocation for the attack). Sony decided to cancel the release without involvement from the US Government. President Obama later termed the move "a mistake" and stated that he wished the head of Sony Pictures would have consulted with him first.[20] But to classify these actions as acts of war would require also classifying the alleged US cyber response and economic sanctions as war. Common sense would dictate that this cyber-attack demands a much different response than if North Korea bombed the Sony building, and calling the hacking incident an act of war confuses the issue. It is difficult to call something a war-winning weapon if its use does not necessarily correspond to a state of war.

Like air power theorists before them, cyber enthusiasts have discovered that the opportunity for an indirect attack, whether it is flying over trenches or sending malicious code

---

[19] Eric Bradner, "Obama: North Korea's Hack Not War but 'Cyber-Vandalism'", *CNN.com*, December 21 2014 http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/ (accessed January 2, 2015)
[20] Ibid.

through Ethernet cables, does not make older ways of war obsolete, but adds other areas to attack and defend. The emotional appeal of easy, dominant victory quickly fades when confronted by technical obstacles and enemy countermeasures. In practice, cyber power is not as quick and effective as advertised, and the mere threat of its use is unlikely to deter potential adversaries. By exposing the logical shortcomings associated with the panacea fallacy, strategists are less likely to rely on a costly, ineffective equivalent to strategic bombing in cyberspace. But as naval commanders found out in WWII, assuming away the unique characteristics of a new domain has consequences as well.

CHAPTER 3: THE UNDERSEA DOMAIN CASE STUDY – A STRATEGY NEGLECTED

This chapter highlights the square peg fallacy by comparing the fleet engagement role U.S. Naval planners intended for submarines prior to the Pearl Harbor attacks to the commerce raiding mission the submarines eventually fulfilled. All combatants, even the Germans who pioneered unrestricted submarine warfare in WWI, underrated the potential to conduct operations under the surface without control of the sea above. The U.S. submarine fleet's low speed relative to enemy warships and vulnerability after the initial attack made them a poor choice to participate in the decisive engagements called for by the accepted naval theory of the time. But the inherent advantage of stealth and the submarine's concomitant ability to operate without air or sea superiority in enemy waters proved to be a strategic advantage that achieved incremental, but undeniable results. The chapter concludes with an analysis of cyber power's role in Air-Sea battle as evidence of the square peg fallacy in cyber strategy.

Theorists Wanted

The two prominent naval theorists prior to WWI, Alfred Thayer Mahan and Sir Julian Corbett, centered their strategic thought on the concept of control of the seas.[1] While they differed on key ideas such as the relative importance of concentrating naval forces and the dominance of defense versus offense, they both generally emphasized large scale fleet action as the method to achieve control of the seas for warfare and commerce while denying it to the

---

[1] A.T. Mahan, *The Influence of Sea Power Upon History 1660-1783*, (New York: Dover Publications, 1987). Julian S. Corbett, *Some Principles of Maritime Strategy*, Classics of Sea Power Series, (Annapolis, MD: Naval Institute Press, 1988).

enemy.[2] The only alternative, accepted more by Corbett than Mahan, was a "fleet in being" strategy that delayed the decisive battle and conducted commerce raiding as attrition around the edges. But this alternative was seen as only a delaying action and relied on land forces or diplomacy to conclude the conflict.[3] Neither considered how operations below the surface would change the very concept of control of the sea.

Although submarines had been in various stages of development and experimentation since David Bushnell's hand crank-powered *Turtle* in 1776, it was not until 1910 that the submarine emerged an effective warship. In that year, the German Navy launched the *U-9*, which had an operational range of 1000 nautical miles, could remain on station for five days, and carried six fairly reliable torpedoes.[4] The technical advances represented by this submarine marked the real beginning of the undersea domain as a viable venue for warfare. This development was lost on the naval theorists of the day. Mahan died in 1914 and would not live to see submarines used against warships and commercial shipping in WWI. Corbett analyzed the German unrestricted submarine warfare campaign of 1917-1918 in his history of WWI and concluded that it provided further evidence that commerce raiding was not a war-winning strategy.[5] Mahan and Corbett believed that the enemy's battle fleet was his center of gravity in the maritime domain, and strategists in the Interwar period planned to use submarines as a part of the fleet and attack it.

---

[2] Karl Lautenschlager, "The Submarine in Naval Warfare 1901-2001," *International Security*, 11, no. 3 (Winter, 1986-1987): 100.
[3] William Spruance, "The Russo-Japanese War: The Emergence of Japanese Imperial Power," *Journal of Military and Strategic Studies*, 6, issue 3 (Winter 2004): 2.
[4] Lautenschlager, "The Submarine in Naval Warfare 1901-2001," 103.
[5] J. J. Widen, *Theorist of Maritime Strategy: Sir Julian Corbett and his Contribution to Military and Naval Thought*, (Surrey, England: Ashgate Publishing, 2012): 142.

Ironically, it was a leading land power theorist that offered a strategy that, when applied to submarine warfare, would prove devastatingly effective. The undersea domain presented an opportunity for a variation on B. H. Liddell Hart's "indirect approach". Opposing forces had no reliable way of detecting a submerged submarine. Even the most advanced sonar equipment developed during WWII was ineffective beyond a few thousand yards. This opened up avenues of attack that moved under lines of warships and straight to commercial shipping, a different portion of the "vital centers" so beloved by early air power theorists. But at the time, the critical capability was still thought to be enemy warships. Contemporary naval strategists thought of the stealth and surprise offered by the undersea domain only in terms of exposing avenues to attack the opposing fleet. But the technical limitations of submarines would undermine this approach. The vast open spaces of the sea made it difficult to translate Liddell Hart's maneuver warfare maxim of "avoiding strong defensive positions to attack weaker ones" to war at sea. In naval warfare the "positions" are relative to the numbers and capabilities of surface warships and frequently shift over time. The strong maritime defensive positions were the warships themselves, and the vast, unprotected flotilla of ships ferrying war material across the ocean's surface represented the weak defensive positions. But before strategists could embrace the indirect approach of attacking the weaker merchant shipping, they had to realize that the technical limitations of submarines made the direct approach infeasible.

Attacking a warship with a submarine presented several challenges. The first was finding the target. The view from a periscope or even a surfaced submarine provides a line of sight that extends only about 10 miles, and the rudimentary passive sonar systems available at the time did not provide direction-finding capability beyond a few thousand yards. The next

22

issue was achieving firing position, about 1000-2000 yards away and shooting at the warship's beam (center when viewed from the side) to give the torpedo the largest possible target to hit. Battle fleets typically travelled at 2-3 times the speed of a submerged submarine. If the submarine spotted a warship in the distance, it had no way to make up ground unless the warship was already traveling on a course that would cause it to interact with the submarine. So many potential encounters were over before they began and the submarine crew left frustrated as the target ships steamed over the horizon.[6] Finally, the demanding undersea environment and weak propulsion power supplied by batteries while submerged prevented submarines from carrying the heavy armor employed by surface ships, giving them little inherent defense against enemy fire. Their main protection was (and still is) stealth, which disappears when a submarine fires the first torpedo. Early steam-powered torpedoes left a telltale wake leading back to the launching submarine's position. Even with the advent of wakeless torpedoes, the unexpected explosion of a warship traveling with the fleet could usually mean only one thing. The fleet would immediately initiate defensive maneuvers and commence hunting for the submarine, whose firing position had brought them within the effective range of the warship's active sonar. Therefore, a submarine's first strike necessitated a high probability of sinking the target, since it would be hard pressed to stay and fight after the fleet became alerted to its presence. This made submarine participation in fleet-on-fleet action a tough assignment that the submarines were not yet ready to accomplish. But these facts did not fit in with the familiar logic of the square peg fallacy. Only the arduous struggle of renewed war at sea could provide the stimulus for new strategic thought about the most effective use of the undersea domain.

---

[6] Lautenschlager, "The Submarine in Naval Warfare 1901-2001," 106.

The Rejection of Commerce Raiding

When the Germans first attempted unrestricted submarine warfare in WWI, it was out of a sense of desperation more than anything else. The British Royal Navy had bottled up the German High Seas Fleet in the North Sea after the Battle of Jutland (1916), leaving Germany no way to weaken the British blockade. In 1917, Germany commenced a commerce raiding campaign and sunk an average of 614,000 tons of British shipping over a six-month period in an attempt to knock Britain out of the war before the US could enter the conflict.[7] This effort was derailed by raw numbers: Germany had a total of 330 submarines available during the war, and the allies had over 43 million tons of available shipping in their entire fleet before the war broke out and produced 10 million tons more during the war. In total, German submarines sunk 19.9% of all Allied shipping employed in WW1, meaning 80.1% of it arrived at its destination. This was not nearly enough to cut off the sea lines of communication to Britain.[8] This failure was seen by both sides as proof that commerce raiding was an unworkable concept, but it was actually just a problem of scale. As the US and Japan would find out in WWII, geography and economics can make this strategy devastatingly effective.

In the Interwar period prior to WWII, both naval powers that eventually conducted unrestricted submarine warfare downplayed the role of submarines as commerce raiders. Germany's wartime U-boat commander, Admiral Karl Doenitz, cited a naval strategy designed to counter the navies of neighboring continental powers (France and Russia) as the reason for building a balanced fleet with a small U-boat contingent, despite his own early efforts to

---

[7] Lautenschlager, "The Submarine in Naval Warfare 1901-2001," 112.
[8] Ibid., 122.

promote his version of commerce raiding which he referred to as "cruiser warfare".[9] Germany was not anticipating another naval confrontation with Britain, so it devoted considerable resources to build a surface fleet that could counter France and Russia and did not build a large number of submarines. When war with Britain finally arrived, Germany's surface fleet was still no match for British. With land wars still raging and insufficient resources to upgrade their surfaces forces significantly, Germany quickly turned once again to the undersea domain. Although German submarines where among the best available in the word, the raw numbers were even worse for them than in WWI.

Since the Germans evaluated the WWI commerce raiding campaign as a failure, they had few submarines available when it became their strategy *in extremis* in WWII. When Donitz ordered the U-boat fleet to commence wolf pack tactics in November 1940, the Germans averaged only 10 submarines at sea each month.[10] The U-boat fleet eventually numbered over 400 in 1943 and in November that year sunk 743,000 tons of shipping, destroying almost 2% of the entire fleet in a month. This high-water mark came too late to decisively cripple Great Britain. By this point Allied countermeasures such as complete air coverage of shipping routes (closing the "air gap") and improved convoy escorts turned the tide, and the German's tonnage numbers would decline for the rest of the war.[11] By the time the Germans realized how to fight in the undersea domain, the Allied countermeasures had caught up and the advantage was gone.

---

[9] Karl Donitz, "The Conduct of War at Sea", Division of Naval Intelligence: Washington, DC, 1946, 1.
[10] Lautenschlager, "The Submarine in Naval Warfare 1901-2001," 115.
[11] Kennedy. *Engineers of Victory*, 50.

In the United States, the Navy had given no significant thought to submarine operations against anything other than warships. From 1940-1941, 35 of 36 major exercises involving submarines directed the U.S. subs to conduct attacks on groups of warships. Although at high levels, some of the fleet leadership had speculated that unrestricted submarine warfare might come into play against Japan, the fleet had never trained for it. In the immediate aftermath of Pearl Harbor, Chief of Naval Operations Admiral Harold Stark, ordered the service to "Execute against Japan unrestricted air and submarine warfare." That concept was so far removed from U.S. doctrine that many of the submarine commanders were unclear as to what the order meant.[12] Even after this direction was explained and incorporated into revisions of tactical publications, 30% of U.S. submarine attacks in the first six months of WWII were against Japanese warships. The square peg fallacy is difficult to overcome.

Unrestricted Submarine Warfare in Retrospect

Analysis of warfare in the undersea domain shows that the most successful strategy was unconventional in several ways. First, the geopolitical situation on land can be the dominant factor in the success or failure of strategy under the sea. Unlike air power which was assumed to be dominant everywhere, the participation of an industrial giant like the U.S. made the undersea campaigns against the U.K and Japan completely different. Germany was never successful in cutting off Britain because the combined U.S.-U.K. shipping fleet was too large and the capacity to replenish sunken vessels was too great. Convoy tactics and airborne reconnaissance and attack focused on decreasing the number of U-boats and lowering the effectiveness of their attacks. This undoubtedly helped maintain Britain's lifeline, but the U.S.

---

[12] Papadopoulos, "Between Fleet Scouts and Commerce Raiders", 28.

crash program to increase shipping capacity (the Liberty Ship program) also had the significant effect of overwhelming the German submarine force's destructive capability. Despite horrific losses and intense effort, German submarines only sunk 17% of available Allied merchant ships, and the allies built more shipping tonnage during the course of the war than they had on hand at the outset. Japan, on the other hand, had a shipping fleet about 1/8th the size of the allies, was heavily dependent on importing war materials, and had very limited capacity to replace sunk merchant shipping. This situation allowed the US submarine force to destroy 50% of their shipping and significantly degrade the Japanese war economy.[13]

Additionally, the traditional idea of concentrating the fleet does not apply well to the undersea domain. In order to maximize the probability of ambushing a merchant ship, commanders spread their forces to cover the greatest area. Even the feared German wolf packs started out from a picket line position dispersed across a wide front. Once one of the pack members detected a convoy, the captain would call in the others for a simultaneous attack. A strategic dispersal would give way to short periods of tactical concentration.[14] But any attempt to concentrate submarine forces before targets were available only served to open the ocean up and routes to transit merchant ships safely. Mahan recommended against dividing the fleet under almost any circumstances because he believed that the entire naval force was weakened when its full strength was not available. In the antithesis of this idea, the U.S. strategically dispersed the submarine fleet so that individual submarines would typically never see each other and communicated infrequently by radio to converge on high-value convoys.[15]

---

[13] Lautenschlager, "The Submarine in Naval Warfare 1901-2001," 122.

[14] Ibid., 121.

[15] Eugene Fluckey, *Thunder Below*, (Chicago, IL: University of Chicago Press, 1992), 234. This WWII memoir describes the typical operating pattern of a U.S. submarine in the Pacific. Flucky's narrative that spanned five war patrols rarely included operating with another vessel of any type.

Finally, the undersea domain provided a route to attack a different center of gravity in a different way. Commerce raiding set the enemy's economy as the center of gravity, and any interaction with an opposing warship was counterproductive. Unlike the decisive fleet-on-fleet engagements envisioned by Mahan and Corbett, unrestricted submarine warfare worked through attrition over a vast area and a long period of time. Like bombing campaigns against industrial targets, the overall strategic effect was hard to quantify. But the undersea domain provided greater opportunity to distinguish targets of industrial significance. The distinctive silhouette of a merchant vessel on the trade route to Japan viewed from a periscope was a strong indicator of the industrial value of that ship, unlike a nondescript large building in the center of a city viewed from high altitude. There was also fairly strong evidence of success or failure, as many US submarines were able to watch their targets sink below the waves. Conversely, battle damage assessment from aerial bombardment remains challenging to this day.

The CBO also targeted the enemy's morale and will to continue fighting. Unrestricted submarine warfare never had this aim. In theory, attacks on shipping by U.S. submarines could destroy food imports bound for Japan and starve the population. But Japan's major constraints were industrial in nature (petroleum and raw materials). The nation's petroleum supply was so limited prior to the war that further restriction risked significantly degrading their military capability. The perception among military leaders that Japan had to strike before the loss of fuel crippled their armed forces was a major factor in the decision to bomb Pearl Harbor.[16] Some food shortages did occur due to submarine destruction of supporting agriculture

---

[16] Scott Sagan, "The Origins of the Pacific War" *The Journal of Interdisciplinary History*, 18, no. 4 (Spring, 1988): 897.

equipment and fertilizers. The Japanese implemented food rationing like most other WWII participants, and although some malnutrition occurred there was no general famine.[17] The industrial effect of material scarcity far outweighed any effect on the will of the people.

Unlike air power, the increased strategic options provided by submarines were never explored in the Interwar period. Although submarines were a poor match for Mahanian strategy, that strategy was the round hole they were assigned to fit in. Once the Japanese attack on Pearl Harbor decimated the battleship fleet and prevented the pursuit of a decisive engagement, the US embraced a strategy of commerce raiding to attack the Japanese economy while control of the seas was unrealistic. This initial lack of innovation represented the opportunity cost of assuming operations in a new domain would follow the same principles as operations in all others. Early emphasis and tactical development of commerce raiding by the U.S. Navy could have more rapidly cut the supply lines to Japan's war machine. But that would have required seeing beyond the logical fallacy of division and realizing that this new venue for combat presented a new range of possibilities beyond the narrow constructs of the past.

The Square Peg Fallacy in the Cyber Domain – Cyber in Air-Sea Battle

If operating in cyberspace is not a war-winning panacea in and of itself, it must be integrated as a component of the overall military effort. When viewed in this manner, cyber power is especially vulnerable to the square peg fallacy. With the advent of sonar that could detect submerged objects, maritime theorists assumed that if a nation commanded the traditional maritime domain (the surface), by extension they would command the undersea

---

[17] Lizzie Collingham, *Taste of War: World War II and the Battle for Food* (New York: Penguin, 2011), 228.

domain as well.[18] Contemporary strategists are also guilty of misapplying rules and concepts from other domains onto the cyber domain. The development of the Air-Sea Battle Concept is a vivid illustration of this strategic error.

The Air-Sea Battle Concept[19], first advanced in 2013, intended to integrate action in all domains (including cyber) to respond to a strategic problem: anti-access/area denial (A2/AD) weapons, most notably intermediate range missiles capable of targeting high value units like aircraft carriers or bases and staging areas in the theater. This capability has the potential to invalidate strategic assumptions about where forces are safe from attack and starting points for offensive action. The concept's originators trace the idea back to the attack-in-depth philosophy of Air-Land battle, which advocated using deep strike capabilities to degrade rear-echelon Soviet forces in Europe.[20] The significance of the update comes mainly from the shift in geography and the potential adversaries' strategy. The coastal missile technology of China and Iran necessitated adding the maritime domain to the previous Air-Land mix, and those county's investment in A2/AD weapons ironically indicated an application of the very same attack-in-depth philosophy of Air-Land battle towards US forces. Air-Sea Battle addresses these concerns by presenting both an offensive and defensive response to A2/AD, emphasizing the necessity to defend US rear echelon forces.[21] These concepts apply reasonably well to the air, land, and maritime domains, but become problematic when extended to the cyber domain.

---

[18] Kennedy, *Engineers of Victory*, 12.

[19] In January 2015, the Joint Staff changed the name "Air-Sea Battle Concept" to "Joint Concept for Access and Maneuver in the Global Commons (JAM-GC)" to remedy the perception of excluding the Army and the land domain. The concept remains the same and will be referred to by its previous name for ease of reference and clarity.

[20] Air-Sea Battle Office, *Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges.* (Washington, DC, May 2013), 2.

[21] Ibid., 1.

The "area" portion of A2/AD is not particularly relevant to defensive cyber operations. The interconnected nature of the domain essentially invalidates the idea of a rear echelon force from the defensive perspective. A computer network onboard an aircraft or ship is not significantly more secure from cyber-attack off the coast of Florida than it would be off the coast of Iran. The underlying goal described in Air-Sea Battle is that computer networks associated with military units will operate securely and be highly resistant to intrusion, which is the goal of US cybersecurity as a whole. The cyber domain represents a route for adversaries to degrade the effectiveness of US forces in an indirect manner, far from the front lines and without direct kinetic attack. But acknowledging that an adversary might take this route to make power projection more difficult is no more significant than acknowledging that they might intercept and try to decode radio transmissions to anticipate ship movements, a tactic dating back almost one hundred years. Dealing with potential cyber-attacks is now one of the basic prerequisites for operating a computer network, and associating this continuously ongoing process with attempts to deny access to a specific geographic area confuses the issue.

Air-Sea Battle's concept of offensive cyber operations presents additional problems. When discussing the need for cross-domain integration, the writers state that "cyber or undersea [as in Tomahawk Strike] operations can be used to defeat air defense systems . . .".[22] While this statement could potentially be true, the results and probability of success are vastly different between a cruise missile strike from a submarine and a cyber-attack targeting air defense networks. Equating the two is a prime example of the square peg fallacy. Assigning the role of protecting attacking US fighter aircraft to cyber forces is a mission for which they are not necessarily ready or suited for, much like assigning WWII submarines to fleet-on-fleet

---

[22] Air-Sea Battle Office, 5.

engagements. This strategy ignores both the drawbacks and unique strengths of operations in the cyber domain.

The method the Air-Sea Battle concept advocates for disrupting air defenses (or other A2/AD weapons) using the cyber domain would most likely be a zero day vulnerability, defined as a software vulnerability that is unknown to the system user or manufacturer.[23] Less sophisticated methods, such as distributed denial of service (DDOS) attacks, would probably be ineffective due to the minimal connections between modern air defense systems and the Internet routes required to flood the network with the requests necessary to take it offline. The potential for strategic use for zero day vulnerabilities can be thought of in terms of two variables: stealth and persistence.[24] Stealth in this context refers to the ability of the cyber-attack to remain undetected once initiated and maintain its use for future attacks. The Stuxnet attack that caused extensive centrifuge damage in Iran's uranium enrichment facilities is an example of an attack with high stealth, as it operated undetected for 17 months. Iran's retaliatory cyber-attack on American and Saudi oil processing facilities' computer networks exhibited low stealth, with detection and cleanup complete within four days.[25] Related to stealth, persistence can be thought of as the "shelf life" of a zero day vulnerability. It is the probability that the vulnerability remains in the system undiscovered by the user or manufacturer. Stuxnet had low persistence since it relied on a combination of four zero day vulnerabilities, any one of which would have stopped the attack if it had been corrected. The DDOS methods North Korea has used to conduct cyber-attacks in South Korea in 2009 and

---

[23] Patti Stockton and Michelle Golabek-Goldman, "Curbing the Market for Cyber Weapons," *Yale Law and Policy Review*, 32, issue 1 (Fall 2013): 240.
[24] Robert Axelrod and Rumen Iliev, "Timing of Cyber Attacks," *Proceedings of the National Academy of Science of the United States of America*, 111 vol. 4 (January 28 2014): 152.
[25] Ibid., 163.

2013 (and allegedly by the U.S. in 2014 in response to the Sony Hack) had high persistence, since the infected computers (bots) are difficult to detect and can be reconstituted using completely different machines for subsequent attacks. This makes correcting the vulnerability very challenging, even when the user knows it is there. The stealth versus persistence considerations lead to significant issues when integrating offensive cyber operations into overall strategy.

The objective of Air-Sea Battle is to mitigate the threat of anti-access weapons and allow high value units to operate in all areas required. But the offensive cyber capabilities required to degrade these weapons would need to have high stealth (to prevent the enemy from immediately deploying other measures once the A2/AD system is compromised) and high persistence (to remain dependable for planning purposes). The unpredictable nature of zero day vulnerabilities can mean that an attack method that is devastatingly effective one day can be rendered useless the next by a simple software update. In the "ends-ways-means" equation, this particular means can be effectively taken away without the commander's knowledge. Like the use of submarines in major fleet engagements, inclusion of offensive cyber operations into the overall strategy is a mission for which the force is not ready.

Contemporary strategic thought on the cyber domain demonstrates aspects of the square peg fallacy. The concepts of stealth, persistence, and the inapplicability of geography-based ideas are domain-specific complexities easily glossed-over by the fallacy of division. Although it is easier to translate assumptions from old domains to new, strategists must thoughtfully consider the benefits and drawbacks of operations in cyberspace to avoid falling prey to fallacious logic.

CHAPTER 4 – RECOMMENDATIONS AND CONCLUSION

This chapter provides a perspective on how the panacea and square peg fallacies are at work in the cyber domain, and recommendations on how to counter their negative influence on strategy.

Recommendations

An Appropriate Doctrinal Home for Cyber Defense

The vast majority of US cyber operations are defensive in nature. Instead of incorporating this defensive effort into a concept like Air-Sea Battle, its logical classification is as a part of the joint function of Protection. Resistance to cyber-attack is just another way of preserving the joint force's fighting potential. The service-specific cyber components are responsible for protecting their networks. This should be thought of as an ongoing process similar to force protection.

The Cyber-Attack Will Not Always Get Through

US cyber strategy should draw a distinction between military and civilian network defense. Although these networks interconnect at thousands of points, the military's primary responsibility should be to defend military capabilities. Critical infrastructure like power plants and commercial air travel are protected by civilian authorities outside of the cyber domain, not by the military. Transportation Safety Administration agents at airports and security guards at power plants are not members of the military. The military defends the physical borders of the nation, which have no counterpart in the cyber domain. The National Security Agency (NSA), the Department of Homeland Security, and law enforcement

organizations like the FBI should defend the information systems that support the economy and power grid; the US government should regulate their design and operation in a way that minimizes vulnerability. The cyber-surveillance functions that the military and the NSA perform may turn up indications of impending attacks like the Sony hack, but these should be turned over to the appropriate civilian authorities for action. The Obama Administration authorized $35 million in 2015 to create the Cyber Threat Intelligence Integration Center, an organization designed to fulfill this need.[1] Just like Douhet's assumptions faltered when it became apparent that not all land had to be defended from air attack at all times, cyber defense becomes more manageable when centered on critical systems. The attack on Sony, while startling to the public and damaging to the company, had no effect on the critical infrastructure of the nation. But by refining methods to pass information to private companies, the U.S. can degrade the ability of rouge nations to embarrass the government through cyberattacks on high-profile corporations.

Not Too Powerful to Be Used

The U.S. government currently controls offensive cyber operations in a manner similar to the release authority for nuclear weapons, a relic of the "mutually assured cyber destruction" concept derived from the panacea fallacy. This unwieldy process consumes significant time and resources from senior leadership. A more efficient command and control system exists in the world of special operations. Theater commanders can approve special operations in an active conflict (e.g., high-value target raids in Afghanistan), whereas covert operations in other

---

[1] Dustin Volz, "What a New $35 Million Agency Is Expected to Do for US Cyber Defense", *Defense One Online*, February 10, 2015, http://www.defenseone.com/technology/2015/02/what-new-35-million-agency-expected-do-us-cyber-defense/105048/ (accessed February 13, 2015).

nations like the Bin Laden into Pakistan raid must gain approval from the highest levels of government. The Department of Defense should also provide tiered approval levels for the range of cyber operations to allow theater commanders to use cyber power efficiently as a part of the overall war effort.

A Strategy of (and against) Dispersion

Much of the focus in cyber warfare has been its application in major state-on-state conflicts. The same factors that make cyber operations difficult against modern adversaries (stealth and persistence) are uniquely suited to countering terrorists and non-state actors. In the ongoing conflict against the Islamic State, the cyber domain has been used to distribute propaganda (decapitation videos) and to provide funding from states and individual donors. The networks facilitating these transactions are susceptible to distributed denial of service and other highly persistent means. US cyber power would be quite effective in interdicting these transactions. Additionally, cyber means are effective against geographically dispersed opponents (i.e. individual members of a terrorist cell connected via the internet) in ways that traditional methods like air power are not. These efforts are most likely in progress behind the scenes, but a clear strategic focus on this line of effort would serve to bring the disparate government organizations (both in and out of the military) together towards a common purpose. By thinking of the cyber domain as analogous to the other domains and looking for its application in future state-on-state wars, the military is missing opportunities to further the goals of the nation in the present conflicts against transnational threats.

Conclusion

Logical fallacies continue to haunt strategic thought because of the sheer difficulty of strategy itself. The multitude of variables and considerations inherent to strategy development make it quite appealing to pick one concept as supremely dominant over all others. This appeal to emotion is exemplified by the panacea fallacy. Similarly, it is much easier to assume that what works in one domain will work in related areas of a different domain. The square peg fallacy evens out those troublesome differences by mistakenly seeing discrete portions of the strategic environment as identical parts with the same properties as a homogenous whole. Some assumptions are necessary for strategy development, but fallacious logic can obscure key factors that represent the difference between victory and defeat.

From a strategic perspective, both the use of Stuxnet and the Sony Pictures hack can be classified as actions taken by governments against civilians in another nation to achieve an indirect effect. This type of action was analogous to strategic bombing and unrestricted submarine warfare. In the cyber domain, the effect of Stuxnet was to set back or slow the Iran nuclear program. For Sony, the effect was raising the relevance of North Korea and reinforcing the regime's power over its people. In the air domain, strategic bombing never lived up to expectations that it would make land operations obsolete. In the undersea domain, the strategy of unrestricted submarine warfare saw action as a second choice three times in history and worked once. Neither of these domains ended up being the definitive in which to solve strategic problems. Even general effectiveness and contribution to overall success is highly variable based on situationally dependent factors (e.g., intelligence for cyber and air, geography for commerce raiding).

Cyberspace must serve as a venue for attack and defense in future conflicts, but in the end it is not a panacea, only another place to fight. On the one hand, the US could be caught chasing the elusive "cyber solution", an optimistic concept that eventually over-promises and under-delivers. On the other hand, forcing cyber concepts into existing military strategies could marginalize the unique aspects of cyber warfare. One side may have the advantage over the other in cyber, but in war the overall winner emerges from the results of conflict in all domains.

BIBLIOGRAPHY

Axelrod, Robert and Iliev, Ruben. "The Timing of Cyber Conflict," *Proceedings of the National Academy of Science of the United States of America*, Volume 111, Number 4, January 28, 2014: 152.

Bradner, Eric. "Obama: North Korea's Hack Not War but 'Cyber-Vandalism'", CNN, December 21 2014 http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/ (accessed January 2, 2015)

Bonner, E. Lincoln III. "Cyber Power in 21st Century Joint Warfare," *Joint Forces Quarterly*, Issue 74, 3rd Quarter 2014: 72.

Bumiller, Elisabeth and Shanker, Thom. "Panetta Warns of Dire Threat of Cyberattack," *New York Times*, October 11, 2012.

Clarke, Richard and Knake, Robert. *Cyber War,* New York: HarperCollins, 2010.

Collingham, Lizzie. *Taste of War: World War II and the Battle for Food*, New York: Penguin, 2011.

Corbett, Julian S. *Some Principles of Maritime Strategy*, Classics of Sea Power Series, Annapolis, MD: Naval Institute Press, 1988.

Crosston, Matthew D. "World Gone Cyber MAD," *Strategic Studies Quarterly*, 5, issue 1, Spring 2011: 100.

Commander Submarine Forces. *Undersea Warfighting*, Norfolk, VA, July 2011.

Damer, T. Edward. *Attacking Faulty Reasoning: A Practical Guide to Fallacy-Free Arguments (Seventh Edition)*, Boston, MA: Wadsworth, 2013, 44-56.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*", Washington, DC, 2011.

Douhet, Giulio. *The Command of the Air*, translated by Dino Ferrari (Washington, DC: Office of the Air Force History, 1983, originally published 1942).

Doenitz, Karl. "The Conduct of War at Sea", Division of Naval Intelligence: Washington, DC, 1946.

Elleman, Bruce and Paine, S.C.M, editors. *Commerce Raiding: Historical Case Studies 1775 -2009*, Newport, RI: Naval War College Press, 2013.

Fluckey, Eugene. *Thunder Below,* Chicago, IL: University of Chicago Press, 1992.

Gartzke, Erik. "The Myth of Cyberwar", *International Security,* 38, no. 2 (Fall 2013): 58.

Gray, Colin. "Making Strategic Sense of Cyber Power: Why the Sky is Not Falling," Carlisle, PA: Strategic Studies Institute and US Army War College Press (April 2013).

Harvey, A. D. "Air Power in Perspective", *Air Power History*, (Fall 2013): 6.

Holmes, James. "Hail to the Deep", *The National Interest*, (July/August 2014): 67-75.

Howard, Michael "Military Science in the Age of Peace,*" RUSI,* March, 1974.

Jacobs, W. A. "Strategic Bombing and American National Strategy, 1941-1943" *Military Affairs,* 50, no. 3 (1986): 137.

Kennedy, Paul. *Engineers of Victory,* New York: Random House, 2013.

Kim, Jack. "North Korea Blames US for Internet Outages, Calls Obama 'Monkey'", *Reuters*, December 27, 2014. http://www.reuters.com/article/2014/12/27/us-northkorea -cybersecurity-idUSKBN0K502920141227 (accessed January 2, 2015)

Lautenschlager, Karl. "The Submarine in Naval Warfare 1901-2001" *International Security*, 11, No. 3 (Winter, 1986-1987): 94-140.

Lonsdale, David J. *The Nature of War in the Information Age,* New York: Frank Cass Publishing, 2004).

Libicki, Martin C. "Why Cyber Will Not and Should Not Have Its Grand Strategist", *Strategic Studies Quarterly*, 8, issue 1: 32.

Mahan, A.T. *The Influence of Sea Power Upon History 1660-1783*, New York: Dover Publications, 1987.

Meilinger, Phillip, editor. *The Paths of Heaven: The Evolution of Airpower Theory,* Maxwell AFB, AL: Air University Press, 1997.

Murphy, Dennis "Pentagon Budget 2015: DoD Cyberspace Operations would get 8.5% Boost", *Janes*, March 16, 2014 http://www.janes.com/article/35427/pentagon-budget-2015-dod cyberspace-operations-would-get-8-5-boost (accessed February 23, 2015).

Murray, Williamson and Millet, Alan editors. *Military Innovation in the Interwar Period.* Cambridge: Cambridge University Press, 1996.

Panetta, Leon, *Remarks by Secretary of Defense Leon Panetta to the Business Executives for National Security* (Washington, DC: Office of the Secretary of Defense, October 11, 2012), http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5136; (accessed October 6, 2014).

Papadopoulos, Randy. "Between Fleet Scouts and Commerce Raiders", *Undersea Warfare,* 7, no.4, (Spring 2005): 28.

Paramore, Woody "The Combined Bomber Offensive's Destruction of Germany's Refined Oil Industry" *Air and Space Power Journal,* (March-April 2012): 73.

Sagan, Scott. "The Origins of the Pacific War", *The Journal of Interdisciplinary History,* 18, No. 4, (Spring 1988): 897.

Sanger, David E. and Perlroth, Nicole. "US Said to Find North Korea Ordered Cyber Attack on Sony", *New York Times,* Dec 17th, 2014.

Spruance, William. "The Russo-Japanese War: The Emergence of Japanese Imperial Power," *Journal of Military and Strategic Studies,* vol. 6, issue 3 (Winter 2004): 2.

Stockton, Patti and Golabek-Goldman, Michelle. "Curbing the Market for Cyber Weapons", *Yale Law and Policy Review,* 32, issue 1 (Fall 2013): 240.

US Joint Chiefs of Staff. *Joint Operations Planning,* Joint Publication 3-0, Washington. DC: Joint Chiefs of Staff, 11 August 2011.

US Joint Chiefs of Staff. *Information Operations,* Joint Publication 3-13, Washington, DC: Joint Chiefs of Staff, 27 November 2012.

Vacca, W. Alexander. "Military Culture and Cyber Security" *Survival,* Vol. 53 Issue 6 (2012): 159-176.

Volz, Dustin. "What a New $35 Million Agency Is Expected to Do for US Cyber Defense", *Defense One Online,* February 10, 2015,http://www.defenseone.com/technology /2015/02/ what-new-35-million-agency-expected-do-us-cyber-defense/105048/ (accessed February 21, 2015).

Widen, J. J. *Theorist of Maritime Strategy: Sir Julian Corbett and his Contribution to Military and Naval Thought,* Surrey, England: Ashgate Publishing, 2012.

VITA

Lieutenant Commander John Witte is a career submarine officer. He was commissioned in 2000 following graduation from Iowa State University. LCDR Witte's first assignment at sea was as a division officer on the fast attack submarine *USS ALBUQUERQUE* (SSN 706) based in Groton, CT. While onboard, he completed an Engineered Refueling Overhaul and a CENTCOM deployment. He went on to serve as Engineer on the guided missile submarine *USS MICHIGAN* (SSGN 727)(Gold Crew) based in Bangor, WA. During his tour, he completed two Western Pacific deployments, including integrated support of naval special warfare. His most recent sea duty was as Executive Officer onboard the fast attack submarine *USS MINNESOTA* (SSN 783) based in Norfolk, VA. During his time there, the ship completed the new construction process through commissioning and initial sea trials. LCDR Witte also served on the staff of Submarine Squadron One as the Naval Special Warfare Planning Officer and on the US Fleet Forces Command Nuclear Propulsion Examining Board. He is a graduate of Old Dominion University with a Master's Degree in Engineering Management. LCDR Witte resides with his wife, Lisa, and children, Logan and Olivia, in Chesapeake, VA.